Seeking Suitable Options for Importing Data from the European Union

ROSA BARCELÓ*

One of the most important issues that a U.S. company operating in the European Union (EU) faces regarding data protection is the problem of transferring European individuals' private data to the United States. This is because the different Member States of the EU have legal regimes that restrict companies from transferring personal data, both on- and off-line, to countries outside the EU that do not provide "adequate" protection for such data.

However, data transfers are permitted under certain circumstances, and those wishing to transfer data to the United States must identify the most appropriate basis for lawful data transfer. One avenue worth exploring is using the U.S. Department of Commerce's safe harbor principles, which renders legal data transfers from the EU. Other alternatives exist whereby data can be transferred lawfully to the United States, and these should not be overlooked. For example, the data exporting company may obtain the individual's consent to the transfer of his/her data, or the EU exporters of private data and the U.S. importer may use the standard contractual clauses recently approved by the European Commission, which ensure an adequate level of protection for the transferred data. Any of these options would allow the transfer of private data to comply fully with EU privacy laws but, as explained in this article, the exporter and importer, in light of their particular needs, should carefully assess the choice of a solution and the specific circumstances surrounding the data transfer.

This article seeks to provide the U.S. importer of private data with a comprehensible overview of the available solutions for importing data into the United States, and ultimately to help them make the optimum choice for the particular data transfer. Toward this end, after a brief introduction, we will look at each possibility for importing data and review, among other things, the obligations that each entails, the competent enforcement bodies, and the likelihood of enforcement actions and penalties. In doing so, we look into practical questions such as the content of a consent form that an individual would execute to permit

*Dr. Rosa Barceló is an associate at Morrison & Foerster (Brussels) and an Adjunct Professor of Law at the University of Namur in Belgium. Dr. Barceló specializes in European legal issues related to electronic commerce, data protection, and intellectual property.

the transfer of his/her data, whether consent to the data transfer must be opt-in or opt-out, whether the U.S. importer could subscribe to the safe harbor principles only for certain types of data imported from the EU but not for others, and which types of data could be imported on the basis of the existence of a sales contract. The two final sections compare the four solutions, focusing on the differences between the safe harbor principles and the standard contractual clauses adopted by the Commission. The article concludes by illustrating several recurrent types of data transfer and suggests reasons that may justify the choice of a particular legal option.

I. The Prohibition on Data Transfers and Exceptions: The Background

The EU Data Protection Directive (Directive)[1] and Member State laws that implement the Directive[2] lay down certain rules that must be respected by those engaged in the processing of private data in order to ensure the protection of such data and thus preserve the privacy rights of European citizens.[3]

These rules require, *inter alia*, the so-called data controller (the person who decides how to carry out the data processing and what to do with the private data) to inform the individuals to whom the data refer of the purposes for the collection of such information. In certain cases, they require the individual's consent for such processing, as well as the possibility for the individual to have access to the data and the right to rectify the data if it is found to be incomplete or inaccurate. The Directive also requires data controllers to apply security measures to prevent unauthorized use or accidental loss of personal data. Under most Member State laws, the start of data processing activities must be reported to the local data protection authority where the data controller is established.

The Directive stipulates that a data controller is allowed to commission another person (referred to as a data processor or agent) to perform specific tasks with the private data on the controller's behalf. For example, a data processor could be in charge of maintaining a database of private data and of contacting individuals for marketing purposes on behalf of the data controller. Regarding human resources data, it is quite common to outsource payroll processing to third parties, who would also be considered data processors. Most of the Directive's rules do not apply to the processor because the data controller remains fully responsible for the data processed on his/her behalf by the data processor, and the data controller must ensure that data processing occurs in compliance with the Directive.[4]

1. Council Directive 95/46/EC, 1995 O.J. (L 281) 31 (discussing the protection of individuals with regard to the processing of personal data and on the free movement of such data).

2. Up to now, all Member States except France and Ireland have implemented the EU Data Protection Directive (Directive); however, both France and Ireland have published implementation draft laws that they intend to adopt during 2003. Copies of the Member State laws that implement the Directive can be found at the EU Commission Web site. Working Party 29, *Status of Implementation of Directive 95 on the Protection of Individuals With Regard to the Personal Data*, *at* http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm (last visited Sept. 18, 2002). Note that Working Party 29 (formally, the Working Party on the Protection of Individuals with regard to the Processing of Private Data, hereinafter "WP 29" or "Working Party 29") is a body competent for interpreting the provisions of the Data Protection Directive. It carries out this task by issuing recommendations, opinions, and working documents on different aspects of the Directive.

3. Pursuant to article 2 of the Directive, data processing means any operation carried out upon personal data, from simple collection to storage, adaptation, making available, transmission, etc. Council Directive 95/46/EC, *supra* note 1, art. 2.

4. Article 17.3 of the Directive sets forth the obligations of the data processor. The relationship between the data controller and the data processor must be documented in a so-called processor agreement. The

A. Articles 25 and 26 of the Directive

One of the most controversial provisions of the Directive is embodied in article 25, which deals with the transfer of personal data to countries outside the EU.[5] According to article 25, private data gathered in EU Member States may not be transferred to another country (outside the EU) where the legal regime does not meet an adequate level of privacy protection for natural persons.[6]

The European Commission may find that a third country does ensure an adequate level of protection, thus allowing data transfers to take place freely to that country.[7] Until now, the Commission has approved transfers to the following countries: the United States (but only to companies that abide by the safe harbor principles),[8] Switzerland,[9] Hungary,[10] and Canada.[11] Argentina, and New Zealand are now under consideration by the Commission.[12]

Thus, the data exporter who wishes to transfer data to a third country must first discover whether the legal regime of that country has been deemed to provide an adequate level of privacy protection. However, if this is not the case, it does not mean that the intended data transfer is frustrated. This is because the company can still try to comply with one of the conditions set forth in article 26 of the Directive to render the transfer lawful. The most relevant exceptions to the prohibition are the following: (i) the data exporter obtains unambiguous consent by the individual to the data transfer; (ii) the transfer is necessary for the performance of a contract between the individual and the company (or the transfer is necessary for the performance of a contract concluded between a third party and the company for the benefit of the individual); and (iii) the organization has put in place safeguards by entering into an agreement, either *ad hoc* or using the Commission's Standard Contrac-

---

agreement must establish the obligations of the data processor, including the particular tasks in relation to the private data as well as the processor's obligation to implement technical and organizational measures to protect the data against destruction, theft, loss, etc. *Id.* art. 17.3.

5. While colloquially we refer to countries outside the EU as those countries where the prohibition of data transfer applies, in fact, the prohibition does not apply to the non-EU European Economic Area countries (EEA), Norway, and Iceland. Norway and Iceland have implemented the Data Protection Directive into their own legislation by reason of their obligations under the EEA Agreement.

6. Council Directive 95/46/EC, *supra* note 1, art. 25.

7. *Id.* arts. 25.6, 31.2.

8. Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, 2000 O.J. (L 215) 7, 47 [hereinafter Frequently Asked Questions].

9. Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, 2000 O.J. (L 215) 1.

10. Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary, 2000 O.J. (L 215) 4.

11. Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, 2000 O.J.

12. Article 29 Data Protection Working Party, *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*, *available at* http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wpdocs_2001.htm; European Commission, *Fourth Annual Report on the Situation Regarding the Protection of Individuals With Regard to the Processing of Personal Data and Privacy in the Community and in Third Countries Covering the Year 1999*, *available at* http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wpdocs_2001.htm.

tual Clauses, which affords to individuals whose data is exported from the EU essentially the same rights as they would have under local EU law.[13]

If the prohibition on data transfers set forth in article 25 of the Directive is violated, it is important to note that the violation may not go unnoticed by the EU authorities, for various reasons. One reason is that under most Member State laws, data controllers are required to notify local authorities of international data transfers. The duty to disclose potential international data transfers is part of the general duty of notification for any data processing in which a data controller is engaged.[14] Another reason is because the Data Protection Authorities (DPA) increasingly monitor data processing activities on an *ex officio* basis, and it may be possible that they would discover the data transfer violation. Finally, in some cases such as the transfer of employee data, it would not be unusual for a disgruntled employee to report his/her company's violation of article 25 to the local DPA. Penalties vary from one Member State to another, and could include not only economic but also criminal sanctions.[15]

Before addressing the U.S. safe harbor rules and the substance of the other exceptions listed above for data transfer, the following paragraphs address the issue of who is competent to make the adequacy decision (i.e., to determine whether a particular country provides an "adequate level" of data protection) and in particular whether Member State laws allow the data controller itself to make such a decision.

B. Responsibility For Carrying Out The Adequacy Determination

Undoubtedly, the European Commission has the authority to decide whether a third country ensures an adequate level of protection, and the Commission's decisions are binding on all Member States.[16] As described above, the European Commission has already issued various adequacy decisions.[17] Individual DPAs may also decide that a third country ensures an adequate level of protection. The key question, however, is whether the data controller, the exporter of the data, can perform such an assessment as well.

---

13. Council Directive 95/46/EC, *supra* note 1, art. 26.

14. The obligation to notify exists under Belgian, Dutch, French, Spanish, and U.K. law. In several Member States (i.e., Austria, Denmark, Ireland, Finland, and Italy) the obligation to notify exists but there are certain exceptions. In Germany, Norway, and Sweden it is possible to choose between appointing a privacy officer and notifying DPAs of databases.

15. For example, violators could face maximum penalties of up to USD 220,000 in Germany, USD 400,000 in France and USD 540,000 in Spain.

16. To reach such a decision, the European Commission has to follow a procedure set forth by articles 25.6 and 31 of the Data Protection Directive. The procedure requires the Commission to consult on its draft adequacy proposal with the following three bodies: first, with the Working Party on the Protection of Individuals with regard to the Processing of Private Data (commonly referred to as "Working Party"). The opinion of WP 29 is not binding on the Commission. However, insofar as WP 29 members are representatives of national data protection authorities who ultimately apply privacy laws (including the adequacy decision), they have considerable influence over the Commission's adequacy determinations. Second, it must consult with Committee 31, which is a committee composed of representatives of Member States (normally representatives of the Ministry of Justice). A majority of this Committee must vote favorably on the Commission's adequacy decision. Finally, the Commission must also notify the draft adequacy decision to the European Parliament, which is entitled to assess whether the Commission exceeded the powers conferred on it by the Directive, but which may not judge the adequacy finding itself. *See* D. Alonso Blas, *Towards a Uniform Application of the European Data Protection Rules, The role of the Article 29 Working Party*, Privacy & Informatie, Feb. 2001, at 4–8.

17. In particular, the United States (safe harbor accord), Switzerland, and Hungary.

Indeed, some Member State laws seem to allow data controllers to determine that a particular country provides an adequate level of protection. For example, the United Kingdom Data Protection Act of 1998 and the newly enacted Dutch Personal Data Protection Act of July 6, 2000 are interpreted by the respective local DPA as allowing the data controller to make such an assessment. Of course, this principle applies unless there is a Commission adequacy decision regarding the relevant country.

Under these circumstances, one may wonder whether the data controller will ever want to fulfill one of the previously mentioned requirements/exceptions necessary to transfer the data lawfully. It seems easier to reach the conclusion that the intended destination country is adequate and proceed with the international transfer.

However, relying only on self-assessment involves certain significant risks: if the national data protection agency learns that an individual's privacy rights have been violated in the importer's country, the exporter's assessment is likely to come under rigorous scrutiny by the DPA. Also, if the DPA considers that the importer country's privacy laws fail to pass the adequacy requirement, then the exporting company is likely to be charged with violation of U.K. or Dutch privacy laws for illegal transfer of data to a country which does not provide adequate protection and without having legal grounds (i.e., being able to use one of the exceptions). Furthermore, this outcome can result even if no violation of rights has occurred, simply because at some point national authorities decide *ex officio* or as a result of an individual's complaint that the destination country laws do not ensure the necessary protection. In both cases, the company may be liable for heavy fines, not to mention the effects of any resulting bad publicity.

For those data controllers who are willing to accept the risks of self-assessment, Working Party article 29 (WP 29) issued an opinion addressed to the Commission providing guidelines on how to carry out such an assessment, which will certainly be a useful tool for the data controllers.[18]

II. An Overview of an Adequacy Determination: The Safe Harbor Principles

The European Commission issued an adequacy determination on July 26, 2000 acknowledging that the safe harbor principles provide adequate protection for private data.[19] It recognized that companies willing to abide by such principles would be deemed to meet the adequacy standard and transfers to such companies would be lawful.[20] For the same reason, EU authorities cannot stop a data transfer to such companies in the United States.

To take advantage of the safe harbor, a company must decide voluntarily to rely on the safe harbor, bring itself into compliance with the safe harbor principles and frequently asked

18. *See* Working Party 29, *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* (July 24, 1998), *at* http://europa.eu.int/comm/internal_market/en/ataprot/wpdocs/wp12en.htm.

19. *See* Frequently Asked Questions, *supra* note 8.

20. *Id.* J. Mogg, Director General, Internal Market DG, in a letter to Robert LaRussa, Under Secretary for International Trade, conceded a grace period until July 2001, during which EU authorities agreed to refrain from enforcing the prohibition on international transfer of data. This standstill period was a political rather than a legal commitment, and thus not legally binding on the Member States, although they respected it. The reason behind this grace period was to allow U.S. companies time to adjust their data processing practices to the principles embodied in the safe harbor accord.

questions, identify in its publicly available privacy policies that it adheres to safe harbor requirements, and declare to the U.S. Department of Commerce that it is in compliance with the safe harbor requirements.

A. Obligations that Arise From Subscribing to Safe Harbor

As for the obligations that safe harbor entails for those U.S. data importers who join it, to summarize, the safe harbor principles would require the company to: (a) provide notice to data subjects about the collection of data, its purposes and intended transfers (if any); (b) provide individuals with the possibility to opt out of disclosure of their personal data to third parties and of its use for purposes other than those for which it was initially collected; (c) take reasonable precautions to protect data from loss, misuse and unauthorized use; and (d) ensure that individuals have access on a reasonable basis to all information that might be held about them. Failure to abide by the principles—after having been certified—must be actionable under law or statute as an "unfair or deceptive act."[21]

The above obligations apply only to personal data imported from the EU. They do not apply to personal data obtained from non-European residents such as the data of U.S. residents.

B. Enforcement of Safe Harbor Principles

To date, the competent bodies for enforcing the safe harbor principles are the Federal Trade Commission (FTC) and the Department of Transportation (DOT). A U.S. importer may incur liability if it persistently fails to comply with safe harbor requirements. Persistent failures to comply arise when an organization "refuses to comply with a final determination by any self-regulatory or government body or where such body determines that an organization frequently fails to comply with the Principles to the point where its claim to comply is no longer credible."[22] In particular, EU data protection authorities and self-regulatory bodies that are competent for referring cases of non-compliance to the FTC could initiate a potential action against a U.S. importer, which is committed to reviewing such referrals on a priority basis. If the FTC concludes that there are grounds for concluding that section 5 of the Federal Trade Commission Act has been violated, it may seek an administrative cease-and-desist order or a federal court order prohibiting the challenged practices. The FTC may obtain civil penalties for violations of federal court orders.

It is important to note that before the FTC has reviewed the case, the complaint must first have gone to the organization responsible for hearing complaints and enforcing the principles. The importer chooses this organization. These organizations include self-regulatory bodies such as BBOnline and DPAs. Both organizations would be allowed to impose sanctions of varying degrees of severity, such as issuing a public statement of the non-compliance, removal of the safe harbor seal, compensation for individuals, etc. While companies will be able to choose to cooperate with self-regulatory bodies or with DPAs, the choice does not exist in relation to human resources data. In such cases, DPAs will

21. *See* Yves Poullet, *Les Safe Harbor Principles: Une protection adéquate?* ASBL Droit et Nouvelles Technologies (17 juin 2000), *available at* http://www.jursicom.net/ uni/doc/20000617.htm (last visited Sept. 20, 2002).

22. Frequently Asked Questions, *supra* note 8.

always have authority to hear complaints regarding human resources information, and U.S. companies, in relation to such data, must comply with any advice they provide.[23] Such authority is in addition to the authority that the FTC would have over the same type of data.

From the perspective of the EU exporter of private data, the fact that the U.S. importer has signed up to the safe harbor principles puts him/her in a much more comfortable position than if this were not the case. Indeed, the data exporter is freed from the obligation to comply with one of the legal grounds for data transfer highlighted above (e.g., to obtain consent from the individual), and he/she can proceed to send the data by applying exactly the same criteria as if the data transfer occurred within a Member State of the EU. To some extent, it could be said that the major burdens and obligations in relation to the private data are shifted from the exporter in the EU to the importer in the United States. Also, as we will see below, as opposed to the *ad hoc* contracts or the "Standard Contractual Clauses" solutions, where the exporter remains jointly liable if the importer violates the data subject's private rights, with safe harbor, the exporter is not responsible for potential violations carried out by the data importer.

C. The Issue of Certifying Certain Data Imported from the EU Only: The Special Status of Human Resources Data

With the safe harbor adequacy decision, the EU admitted for the first time the possibility of finding adequate the circumstances of individual companies (those willing to voluntarily agree to the safe harbor principles) rather than the laws of a country as a whole, as a result of the existence of a legal framework deemed to be adequate.

The fact that a company has certified itself as compliant with the safe harbor principles means that all the data that it receives from the EU will be processed in accordance with such rules. The result of such compliance is that the company as a whole becomes eligible for the receipt of data coming from Europe, in other words, the prohibition on data transfers does not apply any longer for transfers to that company.

In this regard, a question has arisen as to whether a company can adhere to safe harbor for only certain types of data received from the EU but not for other categories or groups of data. For example, a company that sells soft drinks in Scandinavia and ice cream in the Mediterranean countries may wish to adhere to safe harbor rules to import private data gathered through the soft drinks business and to obtain opt-in consent from the customer—which is one of the exceptions to the prohibitions on data transfer—for the data gathered through the ice cream business.

As noted above, according to the Directive, the adequacy decision relates to the statute(s) of a country to the effect that transfers to such a country as a whole can occur without any obstacle and EU authorities can assume that such legal framework will provide sufficient guarantees for the data of EU citizens. Once a country's legal framework has been deemed adequate, to a certain extent EU authorities can overlook systematically the legality of data transfers to such countries deemed adequate and afford them the same treatment as if they occurred within the EU. The safe harbor principles, which set forth a system whereby it is

23. *See id.* (further stating that companies importing human resources data must self-certify to the list maintained by the U.S. Department of Commerce).

not the legal framework of a *country* that is deemed adequate but rather the rules governing a particular *company*, constituted an exception approved only after staunch opposition from Member State data protection authorities.[24] If it were to turn out that the adequacy decision does not refer to all the data the company receives, but only to certain data imported from the EU, the basic rationale behind the adequacy rule—which is to treat systematically all the data transferred to certain countries (or companies) as being deemed protected as if they were being transferred to recipients within the EU—would not be justified. Instead, the possibility to adhere only by groups or data shipments would oblige authorities to monitor whether each transfer indeed is as protected as if it were transferred to recipients within the EU, in light of the company's public statements. This would also be highly confusing for the public in general, who would be forced to investigate whether each data transfer was covered by safe harbor. In this regard, one could argue that adhering to safe harbor for certain data may be misleading to EU users, who will likely assume that if a company is applying safe harbor principles, then all data is covered.

For this reason and on the basis of the Directive, which is also the basis upon which the safe harbor was agreed, it does not seem possible for a company in the United States to comply with safe harbor for only certain data transfers received from the EU and use alternative legal grounds for other data transfers (see sections III and IV for a description). Whether U.S. authorities will embrace this argument with the ability to enforce the safe harbor is uncertain. In this regard, it is important that under most circumstances U.S. authorities will have to interpret the safe harbor principles on the basis of U.S. law, "except where organizations have committed to cooperate with European Data Protection Authorities."[25]

While according to the above argument companies are required to join safe harbor with respect to all data received from the EU, there is an exception to this rule for human resources data that is clearly supported by the language of FAQ 6, which states

> Where the organization wishes its safe harbor benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, it may do so where there is a statutory body with jurisdiction to hear claims against the organization arising out of human resources information . . .[26]

The language of this FAQ suggests that the decision to join safe harbor for human resources data is an option that the company must exercise, but not an obligation. Therefore, companies are allowed to decide whether they want to exempt human resources data from compliance with safe harbor principles, and bring such data to the United States using different legal grounds. The web site of the U.S. Department of Commerce shows that many companies have joined the safe harbor, but have decided to exclude human resources data from the scope of their obligations under the safe harbor.[27]

---

24. European authorities competent for such decisions often complained that self-regulation did not meet the minimum requirements to warrant adequate protection. *See generally*, Working Party 29, *Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the United States Government* (Jan. 26, 1999), *at* http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp15en.htm (last visited Sept. 20, 2002).

25. U.S. Department of Commerce, *Safe Harbor Privacy Principles* (July 21, 2000), *at* http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm (last visited Sept. 20, 2002).

26. Frequently Asked Questions, *supra* note 8.

27. Department of Commerce, *Safe Harbor List*, *at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (last visited Sept. 18, 2002).

III. Exceptions to the Prohibition on Data Transfer: Consent of the Data Subject and Performance of the Contract

As explained above, the data exporter who wishes to transfer data to a third country, which has not been deemed adequate (which is the case for the United States, if the importing company has not subscribed to the safe harbor principles), the exporter can still try to comply with one of the conditions set forth in article 26 of the Directive to render the transfer lawful. Below we examine further the main features of each exception to the prohibition.

A. Consent of the Data Subject

1. *Obligation to Obtain Consent and Requirements for the Content of Consent Clauses*

Data transfers may be made when the individual to whom the data refers has consented unambiguously to the transfer of his/her personal data. If the individual whose data is being transferred to the United States has agreed to the transfer, European enforcement authorities may not prohibit the transfer.[28]

In this regard, consent will only be valid if it is fully informed. This means that in order to allow individuals to make a real choice, data exporters will have to ensure that the notice given to individuals is drafted in a way that makes them fully aware that their data will be transferred to a third country where no adequacy determination is in place and that it will not therefore be legally protected according to the same standards that European law affords. Also, the consent must spell out in detail the purposes for which the data is transferred (to which the data subject gives his/her consent).[29]

DPAs will deem the consent void if the purposes for which the data was gathered and transferred were not properly disclosed. The same may occur if the consent was not obtained in the language of the data subjects' country of residence.

2. *The Question of Opt-in or Opt-out*

Another important question is whether unambiguous consent means opt-out or opt-in consent.[30] While the law is not clear, it would appear that most Member States' authorities are leaning towards the requirement of opt-in consent. A recent case involving data transfers from iBazar, a company operating auction web sites in different EU countries, to eBay in the United States, following the acquisition of iBazar by eBay, highlights the trend towards

28. Council Directive 95/46/EC, *supra* note 1, art. 26.1(a).

29. For a comment on the consent as legal ground for transferring data, see Peter Blume, *Data Protection Issues with Respect to E-commerce*, Computer Und Recht Int'l, 2001, at 11.

30. While the underlying concept of opt-in and opt-out consent is used by both the EU Data Protection Directive and Directive 97/66/EC of the European Parliament and the Council of December 15, 1997, concerning the processing of personal data and the protection of privacy in the telecommunications sector (commonly referred to as the "Telecoms Data Protection Directive" or "ISDN Directive"), these directives do not contain precise definitions. However, it could be said that opt-in is interpreted as an affirmative, volitional act carried out by the data subject (for example, clicking on a box to the effect of accepting something), whereas opt-out is understood as the possibility to object, and failure to object is deemed as an acceptance. For example, this will be the case if someone does not "un-click" a box. This will be deemed a passive action and not doing so means that the individual is accepting something.

opt-in consent for data transfers. In this case, eBay wanted to transfer the customer data from iBazar in the Netherlands to the eBay system in the United States. eBay proposed that the transfer be made unless the customer opposed it (i.e., so-called opt-out consent), but the Dutch data protection authority said that the data could only be used in the United States once the customer had given his/her permission, which should be obtained by opt-in consent. In a note to the lawyers for eBay, the Dutch data protection authority emphasized that the ideal would be for the company to obtain opt-in consent from the individual by means of the following statement: "I accept that my personal data and billing information may be transferred to and used in the United States."[31]

3. *The Use of Consent for Human Resources Data*

Recently the existence of a real possibility to make such a choice (i.e., to give consent to data transfer) has been questioned by national data protection authorities in relation to situations where the data subject has a hierarchical relation with the data controller, which is often the case with employers and employees. The concern is that employees cannot freely consent to such transfers because in these circumstances, employees, or future employees, fear that if they do not sign the consent form they will not be hired or will lose their jobs.

The above argument is shared by some DPAs and lately it has been embraced by WP 29,[32] which has emphasized that employees, and much less employment seekers, do not have the opportunity of making a real decision as to whether they accept having their data sent to a third country. The same point has been made by the consultation document adopted by the European Commission on July 31, 2002, where the Commission's Employment & Social Affairs Directorate General discusses a possible need to legislate by means of a Directive on this issue.[33] Until now, the above statements are opinions and are not fully enforceable, but they indicate a trend by the EU and local DPAs towards the opinion that consent to transfer in the employment context is not a valid option.

Of course, if the employer were willing to add a clause in the consent form allowing the employee to deny his/her permission to the transfer of his/her data without any consequences for the employee, then the above arguments would not seem to apply. However, in most cases, the employer is unable or unwilling to offer this option to employees.

4. *Obligations of the U.S. Importer*

Choosing as grounds for legal data transfer the consent of the subject results in the data importer in the United States having very limited obligations in relation to such data and almost no liability vis-à-vis the data subject. Indeed, if the data subject gave consent for the data transfer in relation to certain purposes—as mandated by local data protection laws—the U.S. importer will be able to use the data for any purpose that is not incompatible with

31. Translation of Letter From Dutch Data Protection Authority to eBay Regarding Data Transfers to the US (July 20, 2001), *at* http://www.cbpweb.nl/english/en_ebay.htm.

32. Working Party 29, *Opinion 8/2001 on the Processing of Personal Data in the Employment Context*, *at* http://europa.eu.int/comm/internal_market/en/dataport/wpdocs/wp48en.pdf.

33. The purpose of the document is to consult the social partners, in accordance with article 138, paragraph 2 of the EC Treaty, on the possible direction of a community action in this field. The document has no official reference number and is intended for the social partners at European level. The aim is to seek their views on this matter.

the purpose for which it was collected. The U.S. importer/data controller will also not be obliged to afford rights such as access, choice, or any other right that the data subject may have had under the legal framework of the country where he/she resides. The U.S. importer's position is much more favorable than that of a data controller bound by the Directive, the safe harbor principles or the Standard Contractual Clauses. Further, even if the U.S. importer uses the data for purposes incompatible with the purposes for which the user gave consent, it is unclear whether it would be held accountable. In particular, it is unclear whether a claim by DPAs or data subjects to enforce the relevant European national law would succeed in European courts, or whether a U.S. court would enforce any European award issued against a U.S. importer. The most likely result is that under such circumstances DPAs instead would act upon the EU controller (exporter), who, at a bare minimum, would probably be banned from carrying out other data transfers to the U.S. importer.[34] Thus, while the U.S. importer may be immune to sanctions, the EU exporter may be impeded from continuing to supply information to the infringing importer, which will also ultimately damage the importer.

Although obtaining consent from the individual as a legal ground for transfer has certain benefits (at least to the U.S. importer), it carries with it certain drawbacks. The first is that according to the Directive, consent must be given for certain well-defined purposes, which imposes limits on what the U.S. importer can do with the data. Unless the consent given by the data subject is not drafted properly, that is, in a sufficiently broad way while still adequately specifying the purposes, the data importer will be restricted in what it can do with the data. Second, it is important to note that under most Member State laws, data subjects can revoke consent to the transfer of data. Such action may put the company in a difficult position. This may be the case where the data subject is an employee of the company who is changing his/her decision to allow the company to transfer data to the U.S. headquarters. If the data subject requires his/her data back from the exporter, this would be legally enforced and the exporter would risk significant sanctions for failure to comply with the data subject's request. In addition, especially if the data exporter and importer are unrelated companies, it may present serious practical difficulties for the exporting company to comply with the data subject's demand that his/her data be retrieved from the importer in the United States.

The final disadvantage of consent as a legal ground is the increasing practical difficulty in obtaining full and informed consent. Europeans are increasingly aware that they have certain rights regarding their personal data and are becoming more skeptical about giving broad consent for data processing and further transfer to countries whose legal regimes do not protect their data in the same way as the European law.

5. *Consequences of Failure to Obtain Consent*

If the EU-based data exporter fails to obtain valid consent and it nevertheless transfers data to the United States without any other valid legal basis, it could be sanctioned for violation of the prohibition of article 25 and may be subject to significant economic and criminal sanctions.[35]

34. Even the EU exporter would probably be deemed unaccountable for the unlawful behavior of the U.S. importer.

35. *See supra* note 15 for an illustration of sanctions.

B. Performance of the Contract

According to the Directive, personal data may be transferred to third countries when the transfer is deemed to be "necessary for the . . . performance of a contract" between the data subject and the data controller.[36] A company engaged in the sale of goods in the EU may transfer private data released by customers placing orders if such data is necessary to perform the sales contract. For example, the address of the customer is considered private data that can lawfully be transferred to the United States insofar as it is required by the seller to send the good to the customer.[37]

The need to transfer for the purposes of performing a contract also extends to those cases where an agreement is concluded between an EU data controller and a non-EU third party involving a transfer to the third party if such transfer is carried out in the interest of the data subject.[38] For example, a U.S. company with offices in the EU could use this legal ground to transfer data concerning its EU employees from Europe to a third party company in the United States to enable such company to provide a health or pension scheme to its EU employees.

One of the drawbacks of this solution is that the only data that can be transferred using this legal ground are the data that are absolutely essential for the conclusion or performance of a contract. This requirement is being interpreted very narrowly by DPAs, who insist that this legal basis can only be used to transfer data that is essential for the performance of the contract, but not for other data. For example, in the above hypothesis, the company may legally transfer the name and address of the customer, but it would be unlawful to transfer, for example, the answer to an opinion poll about customer satisfaction with the product.

IV. Contractual Agreements: Ad Hoc Contracts and Standard Contractual Clauses (Controller to Controller and Controller to Processor)

According to the Directive, Member States may authorize a data transfer of personal data to a third country where the legal system does not ensure an adequate level of protection if the exporter and importer adduce adequate safeguards to protect the data once it is exported outside the EU. The most common way to adduce such safeguards for data exporters and importers is by entering into a contract that obligates them to provide adequate safeguards for the transfer of such data.[39] Essentially, the contract identifies a group of data that is being transferred and the purposes for such transmission, and sets forth in detail the rights and obligations of both parties in relation to such data. Thus, if a multinational company wanted to transfer both human resources data and client-related data back to the United States from the EU, it could enter into a contract for each database specifying in each case the purposes, recipients, retention period, etc.[40]

36. *See* Council Directive 95/46/EC, *supra* note 1, art. 26(c).

37. *Id.* arts. 26.1(b), (c).

38. *Id.* art. 26(b).

39. *Id.* art. 26(2).

40. For a comment on the contractual solution as a legal ground for transferring data, see Elizabeth Longworth, Contractual Privacy Solutions, Address Before the 22d International Conference on Privacy and Personal Data Protection, Venice, Italy, Sept. 2000, *available at* http://www.garanteprivacy.it/garante/fro (last visited Sept. 20, 2002).

The content of such contracts can be self-negotiated, in which case DPAs of the country where the exporter is located will decide on a case-by-case basis whether the agreements ensure an adequate level of protection of the transferred data. Alternatively, the exporter and importer can incorporate the Standard Contractual Clauses that have been approved by the Commission, both of which are discussed below.

A. Obligations of the U.S. Importer: Content of the Ad Hoc Contract

While the contract is in principle self-negotiated, under most Member State laws such contracts must be notified to and approved by national DPAs. It is common for such authorities to review the clauses and assess whether they afford the protection that, in their view, is necessary. If not, the authorities will demand amendments to the contract until the desired level of protection is achieved. The procedure by virtue of which a company submits a transfer request to the Member State authorities on the basis of certain contractual arrangements varies among Member States, both in terms of the steps to be followed and the time frame. Approval generally takes a minimum of one to two months, unless the authorities consider that the contract does not meet the minimum standards, in which case it may take much longer.

While the description of the content of such contracts varies from country to country, as a rule of the thumb, DPAs will require the incorporation of obligations in the contract equivalent to those embodied in the data protection law of the country from which the personal data is being transferred.[41] It also requires the contract include provisions, by virtue of which, the data exporter remains responsible for the wrongdoings of the data importer in relation to such data, or incorporate a joint liability provision. Furthermore, authorities will require the law of the exporter's country to apply to the contract and they will insist on a jurisdiction clause ensuring that authorities in the exporter's country will be able to hear potential complaints.

B. The Standard Contractual Clauses Adopted by the Commission

The approval of the contract by individual national authorities is not necessary when the parties sign or incorporate the clauses found in the EU Commission's Standard Contractual Clauses decision into their commercial contracts.[42] Under such circumstances, the exporter

41. The following list is based on the clauses required by the Spanish Data Protection Agency to be contained in such *ad hoc* contracts, as described in the agency's 1999 annual report: Name of exporter and importer of private data; purpose(s) for which transfer is necessary; detailed description of the data that are being transferred; statement that the collection of data carried out by the exporter (established in Spain) complies with the Spanish data protection law, including the registration of the database before the authorities; statement made by the importer acknowledging that the data will be used only for the purposes for which it was transferred and statement by the importer saying that the data will be processed according to Spanish law; statement by the importer that data will not be transferred to a third party without opt-in consent by the data subject; statement by the importer that it will apply security measures to the database as established by Spanish law; both the exporter and the importer will be jointly liable; Spanish authorities will have jurisdiction; the data subject must be able to exercise the right of access, opposition and blocking before the importer of data; the importer states that it will allow the Spanish agency to inspect its databases, upon request; and once the contractual relationship is terminated the importer will delete the data.

42. Commission Decision of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, Under Directive 95/124/EC, 2001 O.J. (L 181) 19 [hereinafter Decision 2001/497]. For a critical comment on the Commission Decision, see Barbara S. Wellbery & Rosa Barceló, *European Com-*

and importer can be sure that their data transfers from any EU Member State will be deemed to provide adequate protection, without the need for any further approval.[43] Further, they will not need approval for such contracts, although in most EU countries the DPAs must still be notified of the contracts.

In choosing whether to use an *ad hoc* contract or the Standard Contractual Clauses, there is little doubt that if the importer transfers data from each Member State, it would be better to use the Standard Contractual Clauses. This is because by doing so the importer will be able to use almost identical clauses in all Member States. Conversely, if the *ad hoc* contract were to be used, the importer would have to implement and comply with fifteen different contracts. Indeed, if a company relies on *ad hoc* contracts, it would have to continue to track the data received from the EU Member States by country of origin so that it can comply with the individual requirements of each Member State. On the other hand, if both parties use the Standard Contractual Clauses, then the parties can choose the mandatory principles in each case (described in the next paragraph), which means that they will be subject to the same obligations in relation to data received from all fifteen Member States.

1. *Obligations of the Data Importer under the Standard Contractual Clauses*

The standard contractual clauses allow the parties to decide whether the data importer will process the imported data in accordance with either the privacy laws of the country in which the data controller/exporter is established, the safe harbor principles,[44] or the Mandatory Data Protection Principles set forth by the Standard Contractual Clauses (Mandatory Principles).[45] For example, if the parties had chosen the data exporter law and if this law was the Spanish law, the importer would have to comply with Spanish Data Protection Act and the Security Regulation, which sets forth the security measures that must be applied to the data.

Should the parties choose to process the data in accordance with the laws of the country in which the data controller is established or with the safe harbor principles, the data importer must, in any event, also agree to comply with various additional data protection principles embodied in the Mandatory Principles (which differ slightly from those embodied in the safe harbor principles). In particular, the most relevant obligations with which the U.S. importer will have to comply are as follows:

(a) The importer must agree that the data transferred to the United States can only be used for the specific purpose for which they were initially transferred.[46] This obligation is more restrictive than the one embodied in the safe harbor principles, because under the latter the importer is permitted to use the information for purposes other than those specified, provided that they are not incompatible with the purpose for which it was originally collected or authorized by the individual.[47]

mission's Model Contractual Clauses: Paving the Way for International Transfers or a New Hurdle? PRIVACY & INFO. L. REP., Mar. 2001, at 9.

43. In some Member States such as Austria, authorization is still required but is quasi-automatic.

44. As long as the data importer is based in the specific third country to which the decision applies and is not covered by the adequacy decision.

45. *See* Decision 2001/497, *supra* note 42, Annex, Clause 5(c).

46. *Id.* app. 2, ¶ 1.

47. The same comment can be made in relation to Member State laws that incorporate the Directive. Indeed, according to article 6b of the Directive, data controllers are entitled to use the collected data for purposes other than those for which the data were initially collected, provided that such secondary uses are not *incompatible* with the use for which the data were initially collected. The Commission has not clarified why the same principle cannot be used in the context of the standard contractual clauses.

(b) The importer must agree to give data subjects access to their data. This differs from safe harbor, where the obligation to provide access to the data subject is not absolute but subject to the principle of proportionality, which would allow a company to refuse access under certain circumstances such as where the cost was disproportionate. Conversely, the right of access embodied in the Standard Contractual Clauses seems to be absolute.

(c) In regard to transfers of data by the data importer to third parties, the data can be transferred to a third party (established outside the EU or in the United States) only where the importer has either obtained the informed consent[48] of the individual, or the third party company becomes a party to the contract between the data exporter and importer.[49]

Other additional obligations to which the data importer is contractually subjected (independently of whether it is subject to the Mandatory Principles, safe harbor, or the exporter's law) include agreement to submit its data processing facilities to audits at the request of the data exporter.[50] It must also accept a joint liability clause for damages caused to data subjects resulting from violation of the provisions of the contract, although importers are exempt from liability if they can prove that the data exporter is solely responsible for any damage.

The contract must contain a third party beneficiary clause allowing a data subject who has suffered damages as a result of violation of contact clauses to file lawsuits against both the exporter and the importer.[51] The data subject must be able to sue either party to the contract (i.e., the data exporter or the data importer) in the courts of the data subject's own country or those of the data exporter, and to pursue mediation[52] or arbitration. The governing law for the contract must be the law of the country of establishment of the exporter in the EU.

2. *Decision on Standard Contractual Clauses for the Transfer of Personal Data to Processors*

As explained in the first section of this paper, the Directive includes the concept of data processors, which are agents that perform specific tasks with the private data on behalf of the controller.

Another important legislative development is the Decision of the Commission on Standard Contractual Clauses for the transfer of personal data to processors (as opposed to controllers).[53] The Decision contains clauses that are designed to be incorporated into an agreement between a data controller established in the EU and a data processor established in a third country that does not provide an adequate level of protection. If adopted by the exporter and importer, a contract complying with the Commission Decision will not need to be approved by national authorities, who will have to recognize it as providing an appropriate level of protection.

48. That is, opt-in consent for sensitive data, and opt-out consent for non-sensitive information.

49. Decision 2001/497, *supra* note 42, app. 2, ¶ 6.

50. *Id.*, Annex, Clause 5. Investigations may be carried out by the exporter itself or by a body selected by the exporter "in agreement with the Supervisory Authority" and composed of independent members with required qualifications.

51. Except for a very few clauses of the contract, data subjects will be entitled to enforce most of the provisions of the contract.

52. A mediation panel will be created by national data protection authorities.

53. Commission Decision of 27 December 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, Under Directive 65/46/EC, 2002 O.J. (L 6) 52.

V. Questions a Company Must Ask Itself When Choosing the Legal Grounds for Data Transfer

Exporters and importers of private data wishing to move private data to third countries need to take into account the above legal options and evaluate which one is more suitable for the particular circumstances surrounding the transfer of data they intend to carry out.

In looking at the above solutions, it is clear that of the five options (i.e., safe harbor, consent, performance of a contract or *ad hoc* or standard contractual clauses), the safe harbor and contractual clauses are solutions that place greater burdens and liabilities upon the data importer. The consent and performance of contract solutions, however, place more burdens upon the exporter, who is fully (and solely) responsible for ensuring compliance with such requirements, and who risks the possibility that the DPAs will prohibit the data transfer or impose various sanctions.

Therefore, from the U.S. importer's perspective, in principle only in those cases where it is concluded that the use of consent or performance of the contract as legal grounds are unworkable would it make sense to evaluate the use of other solutions.[54] Unfortunately for the U.S. importer, there are more and more cases where reliance on consent or performance of the contract for data transfers is not feasible. Indeed, as pointed out above, relying on performance of the contract as a basis for the data transfer only works when there is a real need to transfer certain data to perform a contract, and DPAs are increasingly more severe in assessing the existence of such a need. Further, if they conclude that the need exists, it will be limited to the data that is absolutely essential for the conclusion and performance of the contract. Nor will the consent solution always work. From a marketing perspective, companies may well find it difficult to obtain opt-in consent from their customers after informing them—as they must in order for the consent to be valid—that the data will be transferred to a place "without protection." Moreover, DPAs are increasingly saying that a consent solution is not suitable in cases where the individual is in a position of hierarchy in relation to the data controller, such as in the employment context.

Thus, if neither of these two legal grounds are suitable, the U.S. importer will have to decide whether to subscribe to the safe harbor principles or alternatively to conclude a contract with the EU exporter that provides adequate safeguards for the transferred data. In making this choice the U.S. importer should take into account the following.

First, because the use of the contract solution entails a fair amount of effort (for example, drafting the contract, agreeing on the clauses, and in some cases notifying the contract to the national DPAs), it may not be the most viable means for those who import data from large numbers of EU exporters. In other words, the dynamics of the contractual solution make it unsuitable for numerous data transfers from different data exporters. Importers should also take into account the fact that some exporters will not be willing to enter into an agreement that renders them jointly liable with the importer. In particular, as the exporter is based in the EU, the data subject may feel more inclined to sue the exporter than the U.S. importer, and therefore the exporter may find joint liability with the importer to be unbalanced and unpalatable.

54. Here we have assumed that the company wants to find the most comfortable position, i.e., the one that is less demanding for the company and that leaves the company with more possibilities to use the data and fewer liability risks. Note that the company may prefer other solutions that, although more cumbersome, may have a better effect upon consumers from a marketing perspective.

Second, as for the obligations placed upon the importer described in the above section, the standard contractual clauses place a slightly greater burden upon the U.S. importer than does the safe harbor solution. In particular, the joint liability clause may deter many companies from using this solution, unless the ties between the exporter and importer are relatively close. For example, if the exporter and importer are the parent and affiliates, the joint liability clause may not be as relevant than if the companies did not have any connection.

Third, whereas the use of the contractual clauses does not prevent a company from using consent for one set of data and using the clauses for another set of data, the safe harbor means that the company will apply the safe harbor principles for all the data that it receives from the EU—except for human resources data.

Fourth, a U.S. company joining the safe harbor should realize that it is volunteering to apply certain rules (i.e., the safe harbor principles), which may constitute a competitive disadvantage *vis-à-vis* other U.S. companies. It also means that violation of the rules potentially will be subject to sanctions, and these would be sanctions for behavior that in the United States is perfectly lawful for those companies that have not subscribed to the safe harbor principles.

Fifth, on the enforcement side, it is uncertain which solutions present greater risks. The clauses set forth the possibility for data subjects to sue in the country where the data exporter is established, in accordance with the law and courts of the exporter. Under the safe harbor, the importer will be subject to the jurisdiction of the FTC. There is no precedent to assess which solution is more favorable.

VI. Evaluation of Common Types of Data Transfer

A. Human Resources Data

Multinational companies commonly aggregate employee and/or customer information collected by branch offices scattered throughout the world at one central location for administrative ease.

While some of the data related to employment can certainly be transferred to the parent company where the headquarters is located on the basis that the transfer is necessary to perform the employment contract, most European authorities interpret this exception rather narrowly and do not allow the transfer of information that is not absolutely necessary for the execution of the labor contract.

To collect employee information falling outside the scope of the "performance of the contract" solution, companies may consider using consent. However, unless the exporter is willing to give a real option to employees, such as really allowing them to object to the transfer of their data, this solution will not work because some DPAs would regard the consent as void. This means that the only workable solutions are the safe harbor or the contractual clauses.

Until now there does not seem to have been a clear indication as to which solution is the preferred one. Besides the differences already mentioned regarding both legal grounds, a potential disadvantage of the contract solution is that the purposes of the data transfer must be described completely, and the company will not be able to do anything with the data other than what was agreed in the contract (unless a new contract is signed). Conversely, under the safe harbor the importer will have more flexibility because it will be able to use the data for other purposes, provided that they are not incompatible with the purpose for

which the data were initially transferred. With regard to enforcement actions for human resources data under safe harbor, companies have to cooperate with DPAs responsible to handle complaints from the data subjects and the FTC remains responsible for potential enforcement actions.

B. Data of EU Citizens Hosted by Host Service Providers in the United States

U.S.-based host service providers (ISP) whose servers are based in the United States and who offer their services to EU customers are "transferring data" to such servers in the United States. As some customer databases are likely to contain the customer's personal information, such data transfer is subject to the prohibition on data transfers unless there is an adequacy finding or the data controller can justify the transfer under one of the exceptions.

In this case, the data controller for the data hosted by the ISP is the ISP customer—not the ISP—and it is therefore the responsibility of the ISP customer to ensure that it has appropriate legal grounds for the transfer of the data to the United States. Under most EU Member State privacy laws, the hosting of data on behalf of the "owner" of the data is considered to be a data processing action carried out for the data controller. Thus, the ISP is considered to be a data processor in relation to such data, and the transfer of data to the ISP is also subject to the prohibition on data transfers.

The existence of such a burden upon the ISP customer puts such U.S. ISPs at a competitive disadvantage *vis-à-vis* other ISPs that offer hosting services in the EU. This is because the clients of ISPs whose servers are located in the EU will not need to worry about meeting the legal requirements for international data transfer. The competitive disadvantage is highlighted if one realizes that in many instances, meeting the legal grounds for data transfer is not an easy task. For example, if the ISP customer runs a Web site that sells books and CDs, it will have to give notice to its customers of the fact that their data are being transferred to the United States and it will have to obtain their consent, which may deter some customers from entering into a sales contract through such a Web site.

The customer could enter into an inter-company contract with their U.S. ISPs, providing adequate safeguards for the customers' transferred data. In particular, it would be possible to use the controller-to-processor standard contractual clauses proposed by the Commission or *ad hoc* contracts. However, in both cases, the contract will have onerous clauses that are not likely to be accepted either by the ISP or by its customer.

Taking into account that the problem will arise with each of the ISP's clients who plans to store private data in the space rented from the ISP, the ISP may wish to address their customers' concerns by adhering to the safe harbor principles. In this way, customers will be able to transfer the data to the servers in the United States without any restrictions.

C. Software Product Vendors

Increasingly, vendors of software programs offer their customers not only the product itself but also the possibility to host the product, including personal information that is inserted in such software database products. There are many examples of this practice, such as corporate training and knowledge management software providers who offer the software and the possibility of having such a tool running from a server managed by the company. Also, it is becoming quite usual for high-cost software that performs a variety of corporate-related functions to be offered to customers on a "shared" basis. In other words, the service

provider will obtain the software and the necessary licenses to be able to offer it to numerous small- and medium-sized enterprises.

In these cases, if the hosting services are provided in a third country such as the United States, potential EU buyers of these products will face the restriction on data transfers. In particular, when the buyer is a company that is responsible for the database hosted in the United States, the data transferred will be human resources data and the company will face problems similar to those described under part VI.B.

In these circumstances, the software vendor—who has an interest in removing obstacles to the use of its software—may want to consider joining the safe harbor and thereby removing the transfer limitation that each company will face. Inter-company contracts are also potential solutions, but there may be many EU companies reluctant to enter into agreements which impose upon them joint liability with the importer.

D. The Case of U.S.-based Companies That Gather Data through the Internet

An important type of data transfer occurs when U.S.-based companies gather private data through Web sites available to EU citizens. Perhaps the most renowned case is Microsoft's new Windows XP operating system and its "passport identification system," which enables end users to store personal information such as calendars, contacts, credit cards as well as passwords, so users do not have to re-enter the same data at different Web sites.

There has been much discussion as to whether under these circumstances data processing by U.S. companies falls within the scope of the application of the EU Directive and national laws that implement it, or whether U.S. companies should abide by the safe harbor rules for the transfer to be lawful—or whether such U.S. companies are not bound by any law at all.

The following provides an overview of the state of the debate on this issue and some recommendations as to how to proceed.[55]

1. *The Application of the Directive Versus Application of Safe Harbor Principles*

The Data Protection Directive applies in two main circumstances: (a) if the data processing is carried out in the EU and the data controller is established in the EU, and (b) if the data controller is established outside the EU but equipment is used in the EU for the purposes of processing data.

A U.S.-based company engaged in the collection of EU citizens' data through Web sites normally will not have a data controller (a person who decides the nature and purposes of the data processing) in the EU. Therefore, the Data Protection Directive will not apply to such U.S. companies by virtue of the first criterion noted above. Note in this connection that the presence in the EU of a data controller employed by a subsidiary of the U.S.-based Web site operator will not be sufficient to trigger this basis for application of the EU law to the U.S. company's data collection activities.

With respect to the second criterion for applying EU laws, most Member States have interpreted the use of "equipment" in the EU rather strictly, to mean, for example, that the

55. *See* Rosa Julià Barceló, *Cookies, Profiles, IP Addresses: Pending Issues in Data Protection Legislation*, Informatik, Dec. 2000, at 14; Lee A. Bygrave, L.A., *Determining Applicable Law Pursuant to European Data Protection Legislation*, 16 Computer L. & Security Rep. 252 (2000); Christopher Kuner, *Beyond Safe Harbor: European Data Protection Law and Electronic Commerce*, 35 Int'l Law. 79 (2001); Cécile de Terwangne, & Sophie Louveaux, *Data Protection and Online Networks*, 13 Computer L. & Security Rep. 234 (1997).

controller in a third country must at least own servers or computers in the EU that process data for them to be deemed to "use equipment" in the EU. Merely having a Web site available to EU citizens would not qualify as "using equipment." However, WP 29 has twice expressed the view that the Directive would normally apply where "personal data are collected directly from individuals in the EU by a US organisation that makes use of [means such as cookies] situated in the territory of a Member State."[56] According to this interpretation, the use of cookies by Web sites that enable the collection of data from European users is considered as using equipment within the E.U., thus falling within the scope of the application of the Directive.[57] If a U.S. company uses its Web site to gather data from the fifteen Member States, the above argument would render *each* of the fifteen Member States' laws applicable to its data processing. Such companies would need at least to (a) register in each Member State (if the web site were used in all fifteen Member States); (b) nominate a representative in each country; (c) fulfill very detailed security measures; and of course (d) comply with the information-provision and opt-in requirements.

Insofar as the Directive applies to the collection of data carried out by a U.S.-based organization via the Internet, this processing—according to article 29—is not governed by the safe harbor principles but by the Directive.

With this interpretation, WP 29 intends to ensure that the safe harbor principles, which are less cumbersome than the rules established by the Directive, are not being used inappropriately to replace the Directive. However, the outcome of this interpretation is likely to lead to consequences that are contrary to its initial purpose. Indeed, the aim of WP 29 to protect the privacy of EU citizens might have been better served if it had accepted the application of the safe harbor principles to the transfer of private data collected directly from EU citizens by organizations established in the United States, instead of trying to enforce the Directive in these circumstances. This is because a company that is asked to comply with all fifteen Member State laws for the same data processing may feel compelled simply to ignore the issue and to comply neither with the Directive nor with the safe harbor principles.

Even though the "official" view is one that supports the application of the Directive, in reality it appears that DPAs are not enforcing their national laws against data controllers established only in the United States whose only connection with the EU is via a Web site that gathers private data of EU citizens. Unofficially, many DPAs have said that they do not agree with the view that cookies are equipment, and that therefore the Directive or national laws that implement it should not apply to data processing undertaken through cookies. They have stated that they find it to be an over-application of the Directive. Moreover, even if DPAs wanted to enforce their laws, they would often encounter a real problem in enforcing them against U.S. companies with no assets in the EU. In addition, Member State authorities still lack the necessary resources to monitor national Web sites for com-

56. Working Party 29, *Opinion 7/99 On the Level of Data Protection Provided by the "Safe Harbor" Principles as Published Together With the Frequently Asked Questions (FAQs) and Other Related Documents on 15 and 16 November 1999 by the US Department of Commerce, at* http://www.europarl.eu.int/dg2/hearings/20000222/libe/arts/art29/en/default.htm.

57. *See* Working Party 29, *Privacy on the Internet – An integrated EU Approach to On-line Data Protection* (Nov. 21, 2000), *at* http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37en.pdf. *See also* Working Party 29, *First orientations of the Article 29 Working Party concerning on-line authentication services* (July 2, 2002), *available at* http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp60_en.pdf.

pliance with national laws, much less the sites of foreign companies. However, some have pointed out that DPAs sometimes seem more interested in targeting big U.S. companies first before going after national companies.

In light of the above circumstances, what should a U.S.-based company with a Web site accessible to EU citizens do? It would seldom make sense for such a company to comply fully with all fifteen Member State laws, especially because most DPAs so far have turned a blind eye to data processing through Web sites operated by companies established outside the EU. However, was a U.S.-based Web site company to engage in activities that strayed far from EU data protection law, the danger remains that a European DPA might seek to enforce its law against the U.S. company. This danger is heightened if the organization has operations and assets (including physical establishments) in the EU that could be targeted by national authorities. Therefore, it would be advisable for U.S.-based web sites doing business with EU residents at least to adopt privacy policies that show compliance with the Directive to a significant extent. This would help avoid drawing the attention of EU authorities to the Web sites and it would also be useful in order to present the organization as "privacy friendly" to European customers. Under this solution, the privacy policy should bind companies to the following obligations: (a) obtaining opt-out consent to gather data (although opt-in consent would be better); (b) informing data subjects of what is being done with their data; (c) directing data subjects on where to access their data (providing an e-mail address); (d) informing data subjects that their data will be stored in the United States; and (e) not transferring their data to third parties unless data subjects have given their express consent (at least on an opt-out basis). This solution would not include registering with national agencies (especially insofar as there is no one-stop registration process) or carrying out the security measures required by EU laws.

Another way for U.S. Web sites employing cookies to reduce the risk of enforcement of EU law by European authorities would be to join the safe harbor. Technically, joining the safe harbor would not suffice under the WP 29 opinion described above, because under that opinion, EU law applies directly to U.S. Web sites employing cookies in the EU, and only compliance with EU law (not the safe harbor) will be sufficient. However, as a practical matter, compliance with the safe harbor is likely to dissuade European DPAs from enforcing their laws against such U.S. web site operators. Indeed, many companies under these circumstances are opting for such a solution. Again, this is a choice that the company makes for a variety of reasons, for example, to be perceived as privacy friendly or to be able to show compliance with "something" if the DPAs were in fact to enforce the EU Directive.

VII. Conclusion

Companies engaged in collecting private data in the EU and importing it into the United States or third countries face challenges and complexities in determining the legal ground on which they will transfer such information. As described in this article, the transfer can be based on *ad hoc* contracts, standard contractual clauses, safe harbor, consent, or performance of contract.

To assess which is the best solution, companies will have to carefully examine, in particular, the obligations that each solution entails, and the likelihood of enforcement actions and penalties. These will have to be matched with the specific needs and circumstances surrounding the data transfer, and an assessment must be made on a case-by-case basis.